

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-297820

(43)Date of publication of application : 10.11.1995

(51)Int.Cl.

H04L 9/06

H04L 9/14

G09C 1/00

(21)Application number : 06-091023

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>
TOSHIBA CORP

(22)Date of filing : 28.04.1994

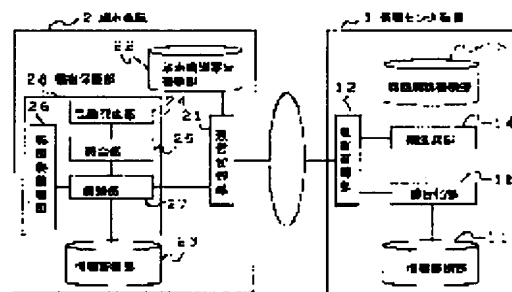
(72)Inventor : YAMANAKA KIYOSHI
KOYAIZU IKURO
KANDA MASASUKI
MATSUDA NOBUHIRO
SEKIYA KUNIIHIKO
YAHATA MEIKI

(54) METHOD AND SYSTEM FOR DIGITAL INFORMATION PROTECTION

(57)Abstract:

PURPOSE: To provide a method and a system for digital information protection system which prevent the illegal use of information without disturbing the privacy.

CONSTITUTION: When information is received from an information center device 1 to a terminal equipment 2, enciphered information is received and is stored in an information storage part 23; and when information is used, random numbers generated by a random number generation part 24 are transmitted from the terminal equipment 2 to the information center device 1 to request a deciphering key for deciphering information, and random numbers and the deciphering key are enciphered by a terminal secret key and are transmitted from the information center device 1 to the terminal equipment 2. The terminal equipment 2 decipheres random numbers and the deciphering key and collates transmitted random numbers and received those with each other; and when they coincide with each other as the result of collation, the terminal equipment 2 decipheres digital information and erases random numbers and the deciphering key.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-297820

(43) 公開日 平成7年(1995)11月10日

(51) Int.Cl. ⁴	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/06				
	9/14			
G 0 9 C 1/00		9364-5L		
			H 0 4 L 9/ 02	Z
審査請求 未請求 請求項の数 3 O L (全 9 頁)				

(21) 出願番号 特願平6-91023

(22) 出願日 平成6年(1994)4月28日

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目1番6号

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 山中 喜義

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(72) 発明者 小柳津 育郎

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(74) 代理人 弁理士 吉田 精孝

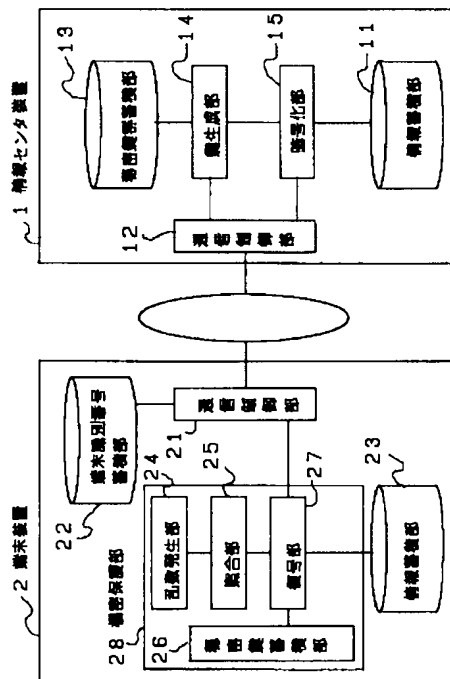
最終頁に続く

(54) 【発明の名称】 デジタル情報保護システム及びその方法

(57) 【要約】

【目的】 プライバシを侵害すること無く情報の不正使用を防止できるデジタル情報保護システム及びその方法を提供する。

【構成】 情報センタ装置1から端末装置2に情報を受信する際には暗号化された情報受信して情報蓄積部23に蓄積しておき、情報を使用する際に端末装置2から情報センタ装置1に乱数発生部24によって発生した乱数を送信して情報を復号する復号用鍵を要求し、情報センタ装置1から乱数と復号鍵を端末秘密鍵によって暗号化して端末装置2に送信する。端末装置2では乱数と復号鍵を復号して送信した乱数と受信した乱数を照合し、照合の結果これらが一致したときにデジタル情報の復号を行い、乱数と復号用鍵を消去する。



【特許請求の範囲】

【請求項 1】 共通鍵暗号方式により暗号化された音声、音楽、映像、文字の少なくとも一つからなるデジタル情報を情報センタ装置から通信回線を経由して受信し端末装置に蓄積して利用の都度、前記端末装置から情報センタ装置に復号鍵を要求するデジタル情報保護システムであって、
 前記情報センタ装置は、デジタル情報を蓄積する情報蓄積手段と、
 端末装置との通信を行なう通信制御手段と、
 複数の端末装置を一意に特定する端末識別番号と端末秘密鍵とを対応させて格納する秘密鍵群蓄積手段と、
 情報の暗号化用鍵及び復号用鍵を生成する鍵生成手段と、
 前記暗号化用鍵を用いてデジタル情報を暗号化する暗号化手段と、
 前記端末装置から要求のあったデジタル情報を前記暗号化手段により暗号化して前記端末装置に送信する情報送信手段と、
 前記端末装置から復号用鍵の要求があったときに、該端末装置から受信した乱数及び前記復号用鍵を該端末装置に対応する前記端末秘密鍵を用いて暗号化して前記端末装置に送信する復号鍵送信手段とを備え、
 前記端末装置は、前記情報センタ装置との通信を行なう通信制御手段と、
 前記端末識別番号を格納する端末識別番号蓄積手段と、
 デジタル情報を蓄積する情報蓄積手段と、
 乱数データを発生する乱数発生手段と、
 前記情報センタ装置に対して前記復号鍵を要求する際に前記乱数データを前記情報センタ装置に送信する復号鍵要求手段と、
 前記発生した乱数データと前記情報センタ装置から受信した乱数データの値を照合する照合手段と、
 端末装置の秘密鍵を格納する秘密鍵蓄積手段と、
 前記照合手段の照合結果に基づいて、前記秘密鍵を用いて前記復号用鍵及びデジタル情報を復号する復号手段と、
 少なくとも前記乱数発生手段、照合手段、秘密鍵蓄積手段、復号手段を秘密保護する保護手段を備えることを特徴とするデジタル情報保護システム。

【請求項 2】 共通鍵暗号方式により暗号化された音声、音楽、映像、文字の少なくとも一つからなるデジタル情報を情報センタ装置から通信回線を経由して受信し端末装置に蓄積して利用の都度、前記端末装置から情報センタ装置に復号鍵を要求するデジタル情報保護方法であって、
 情報要求の際に前記端末装置では、所望のデジタル情報を一意に特定する情報識別番号を前記情報センタ装置に送信し、
 前記情報識別番号を受信した情報センタ装置では、前記

受信した情報識別番号に対応したデジタル情報を情報蓄積手段より取り出し、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した暗号鍵を用いて前記デジタル情報を暗号化して前記端末装置に送信し、

該暗号化デジタル情報を受信した端末装置では、受信した暗号化デジタル情報を情報識別番号と共に情報蓄積手段に蓄積し、

該情報蓄積手段に蓄積された情報を利用するときに、利用したい情報の情報識別番号を前記情報蓄積手段より取り出し、該情報識別番号を、乱数発生手段で発生した乱数及び端末識別番号と共に前記情報センタ装置に送信し、

前記情報識別番号、乱数及び端末識別番号を受信した情報センタ装置では、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した復号鍵を生成すると共に、該端末識別番号に相当する端末秘密鍵により、前記復号鍵と乱数の結合ビット列を暗号化して前記端末装置に送信し、

この後、端末装置では、前記情報センタ装置からの受信情報を予め蓄積されている端末秘密鍵で復号して、乱数と復号鍵を取り出し、該乱数と送信前に端末装置で生成した乱数とを比較し、該乱数が一致した場合のみ、該復号鍵により端末装置の情報蓄積手段内の暗号化デジタル情報を復号することを特徴とするデジタル情報保護方法。

【請求項 3】 前記情報識別番号に加え、端末装置または情報センタ装置で生成した 1 つ以上のパラメータを組合わせた秘密関数で計算した暗号鍵及び復号鍵により、デジタル情報の暗号化及び復号を行うことを特徴とする請求項 2 に記載のデジタル情報保護方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、音楽、映像、プログラム等の暗号化されたデジタル著作物情報を、電気通信網または有線放送網などの公衆網ないし専用網を介して受信して蓄積した後、情報を利用する際に、復号鍵を配送するデジタル情報保護システム及びその方法に関するものである。

【0002】

【従来の技術】近年、音声・動画・静止画等のデジタル情報圧縮技術（例えば、MPEG=Moving Picture Image Expert Group, JPEG=Joint Photographic Expert Group など）、及び ISDN を代表とする高速デジタル通信技術の発達により、音楽・映像・絵画・書籍等の著作物をデジタル情報に変換、圧縮符号化して通信回線を利用して送信することが実現可能となってきた。

【0003】映像等のデジタル情報に比べデータ量の少ないコンピュータソフトウェアでは、既に、パソコン

通信等を利用した配送サービスを実施している例がある。また、米国内において最近サービスが開始されたCD-ROMによるコンピュータソフト販売の方法は、暗号化された販売用ソフト及び暗号化されていないデモ用ソフトを格納するCD-ROMを低価格で販売・配布し、利用者はデモ用ソフトで試用後、購入希望後をサービスセンターに電話で申し込んで復号鍵を受け取る形式をとっている。

【0004】

【発明が解決しようとする課題】従来のパソコン通信などによる、コンピュータソフト販売の場合、ソフトウェアの暗号化がなされておらず、従来のフロッピーディスクなどのパッケージによるソフトウェア販売方法に比べ違法コピーをより容易にさせる環境を提供することになる。また、CD-ROMによる配布の場合は、電話にて復号鍵をセンタより受け取る際に、センタオペレータを介するため、人手がかかり、かつプライバシー侵害の問題が生じる。

【0005】本発明の目的は上記の問題点に鑑み、端末の記録状況がセンタで把握でき、不正コピーを防止するデジタル情報保護システム及びその方法を提供することにある。

【0006】

【課題を解決するための手段】本発明は上記の目的を達成するために、請求項1では、共通鍵暗号方式により暗号化された音声、音楽、映像、文字の少なくとも一つからなるデジタル情報を情報センタ装置から通信回線を経由して受信し端末装置に蓄積して利用の都度、前記端末装置から情報センタ装置に復号鍵を要求するデジタル情報保護システムであって、前記情報センタ装置は、デジタル情報を蓄積する情報蓄積手段と、端末装置との通信を行なう通信制御手段と、複数の端末装置を一意に特定する端末識別番号と端末秘密鍵とを対応させて格納する秘密鍵群蓄積手段と、情報の暗号化用鍵及び復号用鍵を生成する鍵生成手段と、前記暗号化用鍵を用いてデジタル情報を暗号化する暗号化手段と、前記端末装置から要求のあったデジタル情報を前記暗号化手段により暗号化して前記端末装置に送信する情報送信手段と、前記端末装置から復号用鍵の要求があったときに、該端末装置から受信した乱数及び前記復号用鍵を該端末装置に対応する前記端末秘密鍵を用いて暗号化して前記端末装置に送信する復号鍵送信手段とを備え、前記端末装置は、前記情報センタ装置との通信を行なう通信制御手段と、前記端末識別番号を格納する端末識別番号蓄積手段と、デジタル情報を蓄積する情報蓄積手段と、乱数データを発生する乱数発生手段と、前記情報センタ装置に対して前記復号鍵を要求する際に前記乱数データを前記情報センタ装置に送信する復号鍵要求手段と、前記発生した乱数データと前記情報センタ装置から受信した乱数データの値を照合する照合手段と、端末装置の秘密

鍵を格納する秘密鍵蓄積手段と、前記照合手段の照合結果に基づいて、前記秘密鍵を用いて前記復号用鍵及びデジタル情報を復号する復号手段と、少なくとも前記乱数発生手段、照合手段、秘密鍵蓄積手段、復号手段を秘密保護する保護手段を備えるデジタル情報保護システムを提案する。

【0007】また、請求項2では、共通鍵暗号方式により暗号化された音声、音楽、映像、文字の少なくとも一つからなるデジタル情報を情報センタ装置から通信回線を経由して受信し端末装置に蓄積して利用の都度、前記端末装置から情報センタ装置に復号鍵を要求するデジタル情報保護方法であって、情報要求の際に前記端末装置では、所望のデジタル情報を一意に特定する情報識別番号を前記情報センタ装置に送信し、前記情報識別番号を受信した情報センタ装置では、前記受信した情報識別番号に対応したデジタル情報を情報蓄積手段より取り出し、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した暗号鍵を用いて前記デジタル情報を暗号化して前記端末装置に送信し、該暗号化デジタル情報を受信した端末装置では、受信した暗号化デジタル情報を情報識別番号と共に情報蓄積手段に蓄積し、該情報蓄積手段に蓄積された情報を利用するときに、利用したい情報の情報識別番号を前記情報蓄積手段より取り出し、該情報識別番号を、乱数発生手段で発生した乱数及び端末識別番号と共に前記情報センタ装置に送信し、前記情報識別番号、乱数及び端末識別番号を受信した情報センタ装置では、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した復号鍵を生成すると共に、該端末識別番号に相当する端末秘密鍵により、前記復号鍵と乱数の結合ビット列を暗号化して前記端末装置に送信し、この後、端末装置では、前記情報センタ装置からの受信情報を予め蓄積されている端末秘密鍵で復号して、乱数と復号鍵を取り出し、該乱数と送信前に端末装置で生成した乱数とを比較し、該乱数が一致した場合のみ、該復号鍵により端末装置の情報蓄積手段内の暗号化デジタル情報を復号するデジタル情報保護方法を提案する。

【0008】また、請求項3では、請求項2記載のデジタル情報保護方法において、前記情報識別番号に加え、端末装置または情報センタ装置で生成した1つ以上のパラメータを組合わせた秘密関数で計算した暗号鍵及び復号鍵により、デジタル情報の暗号化及び復号を行うデジタル情報保護方法を提案する。

【0009】上記課題を解決するため、共通鍵暗号方式により暗号化されたデジタル情報本体を通信回線利用により配送した後、情報を利用する際に、1回のみ復号可能な復号鍵を通信回線により配送するシステム及び方法に関する。

【0010】

【作用】本発明の請求項1によれば、端末装置から情報

センタに情報を要求する際には、端末装置は、通信制御手段によって情報センタ装置に接続して、必要なデジタル情報を検索し、情報本体の配送要求を行なう。これにより、情報本体の配送要求を受けた情報センタ装置では、要求されたデジタル情報が情報蓄積手段から取り出されると共に、鍵生成手段によって暗号鍵が生成され、暗号化手段により前記取り出されたデジタル情報が該暗号鍵により暗号化されて前記端末装置に送信される。この後、端末装置では、受信した暗号化デジタル情報が情報蓄積手段に蓄積される。該蓄積されたデジタル情報を利用する際には、端末装置では、情報蓄積手段内の情報から利用したい情報が選択され、乱数発生手段により乱数が生成された後、復号鍵要求手段により該乱数が情報センタ装置に送信される。該乱数を受信した情報センタ装置では、鍵生成手段により復号鍵が生成され、復号鍵送信手段によって、端末装置の秘密鍵を用いて、例えば前記復号鍵を乱数のビット単位に連結した結合ビット列が暗号化されて端末装置に送信される。端末装置では、前記情報センタ装置からの受信情報を復号手段で秘密鍵蓄積手段より取り出した端末装置の秘密鍵で復号して、乱数と復号鍵を取り出し、該乱数と送信前に端末装置で生成した乱数とが照合手段によって照合され、この照合の結果、乱数が一致しない場合には、情報の復号が禁止される。また、一致した場合には、復号手段によって該復号鍵を用いて情報蓄積手段内の暗号化デジタル情報が復号された後、前記乱数及び復号鍵が消去される。また、端末装置での、乱数発生手段、照合手段、復号手段及び秘密鍵蓄積手段はすべて保護手段によって封印等されて端末装置の利用者から隔離され、機密保護されている。

【0011】また、請求項2によれば、端末装置から情報センタに対して情報を要求する際には、前記端末装置によって所望のデジタル情報を一意に特定する情報識別番号を前記情報センタ装置に送信され、前記情報識別番号を受信した情報センタ装置により、前記受信した情報識別番号に対応したデジタル情報が情報蓄積手段より取り出され、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した暗号鍵を用いて前記デジタル情報が暗号化されて前記端末装置に送信される。この後、前記暗号化デジタル情報を受信した端末装置では、受信した暗号化デジタル情報が情報識別番号と共に情報蓄積手段に蓄積され、該情報蓄積手段に蓄積された情報を利用するときに、利用したい情報の情報識別番号が前記情報蓄積手段より取り出され、該情報識別番号が、乱数発生手段で発生された乱数及び端末識別番号と共に前記情報センタ装置に送信される。前記情報識別番号、乱数及び端末識別番号を受信した情報センタ装置では、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した復号鍵が生成されると共に、該端末識別番号に相当する端末秘密鍵により、前記

復号鍵と乱数の結合ビット列が暗号化されて前記端末装置に送信される。この後、端末装置では、前記情報センタ装置からの受信情報が端末秘密鍵を用いて復号されて、乱数と復号鍵が取り出され、該乱数と送信前に端末装置で生成した乱数とが比較され、該乱数が一致した場合のみ、該復号鍵により端末装置の情報蓄積手段内の暗号化デジタル情報が復号される。

【0012】また、請求項3によれば、前記情報識別番号に加え、端末装置または情報センタ装置で生成された1つ以上のパラメータを組合わせた秘密関数を用いて計算された暗号鍵及び復号鍵により、デジタル情報の暗号化及び復号が行われる。

【0013】

【実施例】以下、図面に基づいて本発明の一実施例を説明する。図1は、本発明の第1の実施例のデジタル情報保護システムを示す構成図である。図において、1は情報センタ装置で、デジタル情報を蓄積する情報蓄積部11、後述する端末装置2との通信を行なう通信制御部12、複数の端末装置を一意に特定する端末識別番号と秘密鍵の対応を格納する秘密鍵群蓄積部13、共通鍵暗号方式による情報の暗号化および、復号を行なう鍵を生成する鍵生成部14、デジタル情報を暗号化する暗号化部15を備えている。

【0014】2は端末装置で、情報センタ装置1との通信を行なう通信制御部21、端末識別番号を格納する端末識別番号蓄積部22、デジタル情報を蓄積する情報蓄積部23、乱数データを発生する乱数発生部24、乱数データを照合する照合部25、端末装置の秘密鍵を格納する秘密鍵蓄積部26、鍵情報及びデジタル情報を復号する復号部27、前記乱数発生部24、照合部25、秘密鍵蓄積部26、及び復号部27を少なくとも機密保護する機密保護部28である。

【0015】ここで、機密保護部28による機密保護の方法としては、「この部分はユーザが開封することを禁止する」などの注意書きを明記した簡易な封印、カスタムLSIにより物理的に外部から侵害できない専用ハードによる保護（例：R.Mori and M.Kawahara' Supredistribution: The Concept and the Architecture' Trans. IEICE, E-73-No.7, 1990.7）など様々な方法が提案されており、これらのいずれを用いることも可能である。

【0016】次に、前述の構成よりなる第1の実施例において、情報センタ装置1から端末装置2にデジタル情報を受信して端末装置2に蓄積するまでの情報受信・蓄積過程の動作手順を図2に示すフローチャートに基づいて説明する。なお、端末装置2と情報センタ装置1間の回線はISDNなどの公衆通信回線を利用する例で説明する。

【0017】端末装置2は、情報センタ装置1に接続して（SA1）、必要なデジタル情報を検索し、該情報を一意に特定する情報識別番号を情報センタ装置1に送

10

20

30

40

50

信して情報本体の配送要求を行なう（S A 2）。ここで、情報識別番号は、例えば音楽情報の場合、国際レーコーディングコード（I S R C）など、全世界共通コードまたは、該情報提供業者が独自に付与した情報を一意に特定できる番号等である。

【0018】情報本体の配送要求を受けた情報センタ装置1は、情報識別番号に対応したデジタル情報を情報蓄積部11より取り出し（S A 3）、鍵生成部14によって前記情報識別番号をパラメータとする秘密関数により暗号鍵K sを生成し（S A 4）、暗号化部15で前記取り出されたデジタル情報を該暗号鍵により暗号化して（S A 5）、端末装置2に送信する（S A 6）。

【0019】ここで、暗号化アルゴリズムとして、例えばF E A L, D E Sなどの共通鍵暗号方式を使用することができる。また、秘密関数は、情報センタ装置1のみが知っており、端末装置2または端末利用者が入力パラメータから容易に結果を推定できない一方向性関数などである。

【0020】この後、端末装置2では、図3に示すように、受信した暗号化デジタル情報を情報識別番号とともに情報蓄積部23に蓄積する（S A 7）。

【0021】次に、第1の実施例においてデジタル情報を利用する情報利用過程の動作手順を図4に示すフローチャートに基づいて説明する。端末装置2では、情報蓄積部23に受信・蓄積したデジタル情報から利用したい情報を選択し、該情報の情報識別番号を取り出す（S B 1）。次いで、乱数発生部24で乱数Rを生成した後（S B 2）、通信制御部21を介して情報センタ装置1に接続し（S B 3）、前記情報に対応する情報識別番号、乱数Rおよび、端末識別番号蓄積部22より取り出した端末識別番号とともに情報センタ装置1に送信する（S B 4）。

【0022】これらの情報受信した情報センタ装置1では、鍵生成部14により前記受信した情報識別番号をパラメータとする秘密関数で計算した復号鍵K sを生成する（S B 5）。ここで、秘密関数は前記暗号鍵を生成する際に適用した同一の秘密関数である。

【0023】次に、情報センタ装置1は、暗号化部15で、秘密鍵群蓄積部13より取り出した該端末識別番号に対応する端末秘密鍵K iにより、前記復号鍵K sと乱数Rをビット単位に連結した結合ビット列K s || Rを暗号化し（S B 6）、端末装置2に送信する（S B 7）。図5に、情報センタ装置1の秘密鍵群蓄積部13の情報を示す。秘密鍵群蓄積部13には端末識別番号（I D 1, I D 2, …）と端末秘密鍵（K 1, K 2, …）が対になって蓄積されている。

【0024】端末装置2では、前記情報センタ装置1からの受信情報を復号部27で秘密鍵蓄積部26より取り出した端末の秘密鍵K iで復号して（S B 8）、乱数Rと復号鍵K sを取り出し、該乱数Rと送信前に端末装置

2で生成した乱数とを比較する（S B 9）。この比較の結果、乱数が一致しない場合には、情報の復号を禁止する（S B 10）。また、一致した場合には、復号部27で該復号鍵K sにより情報蓄積部23内の暗号化デジタル情報を復号した後（S B 11）、前記乱数及び復号鍵を消去する（S B 12）。なお、端末装置2での、乱数発生、乱数照合、復号処理及び秘密鍵蓄積部はすべて機密保護部28内に封印されて端末装置2の利用者から隔離されている。

【0025】本第1の実施例によれば、情報を利用する際、情報センタ装置から復号鍵を受信して1回だけ復号できるしくみが提供可能である。しかも、乱数を端末装置2で生成して情報センタ装置1に送信した後、情報センタ装置1では復号鍵と乱数に暗号化して端末装置2に返送することにより、端末装置2と情報センタ装置1との間の送受信情報を盗聴して、同一のトランザクションを生成する疑似センタをパソコン等で構成して同一のデジタル情報をセンタ課金なしに不正利用することを不可能としている。さらに、従来のC D-R O Mによる情報の配布等に比べて個人のプライバシーを侵害することもない。

【0026】次に、情報センタ装置1からデジタル情報を受信して端末装置2に蓄積するまでの情報受信・蓄積過程の動作手順の第2の実施例を図6に示すフローチャートに基づいて説明する。ここで、第2の実施例における装置構成は、図1に示す第1の実施例の構成と同様である。また、図2、図3、図4に示した第1の実施例では、各情報識別番号に対して暗号化・復号鍵が一意に定まるのに対して、第2の実施例では、同一情報識別番号であっても異なる暗号化・復号鍵を生成できるように情報識別番号に加え、端末装置2または情報センタ装置1で生成した1つまたは複数のパラメータを組合せた秘密関数で暗号化・復号鍵を計算しており、これにより端末装置2内の情報蓄積部23に蓄積されているデジタル情報の暗号攻撃（暗号解読処理）に対して安全性をより強固にしている。

【0027】図6に示す第2の実施例では、鍵の生成パラメータとして、情報識別番号、端末識別番号及び、送信年月日の3つのパラメータを利用した場合の例で説明する。

【0028】端末装置2は、情報センタ装置1に接続して（S C 1）、必要なデジタル情報を検索し、端末識別番号蓄積部22より取り出した端末識別番号と該情報を一意に特定する情報識別番号を情報センタ装置1に送信して情報本体の配送要求を行なう（S C 2）。

【0029】情報センタ装置1では、前記受信した情報識別番号に対応したデジタル情報を情報蓄積部11より取り出す（S C 3）。次いで、鍵生成部14で前記情報識別番号、端末識別番号及び、作成年月日を組合せたパラメータとする秘密関数により暗号鍵を生成する（S

C 4)。鍵生成用情報としては、受信年月日、端末識別番号以外に情報センタ装置 1 で生成する乱数、作成時刻など様々なものが考えられ、これらを用いることも可能である。

【0030】この後、情報センタ装置 1 は、暗号化部 15 で前記取り出されたデジタル情報を該暗号鍵により暗号化して（SC 5）、情報識別番号、端末識別番号以外の鍵生成用情報（本実施例の場合、作成年月日）と共に端末装置 2 に送信する（SC 6）。

【0031】これらを受信した端末装置 2 では、図 7 に示すように受信した暗号化デジタル情報を情報識別番号、鍵生成用情報（作成年月日）と共に情報蓄積部 23 に蓄積する（SC 7）。

【0032】次に、第 2 の実施例においてデジタル情報を利用する情報利用過程の動作手順を図 8 に示すフローチャートに基づいて説明する。

【0033】端末装置 2 では、情報蓄積部 23 に受信・蓄積したデジタル情報から利用したい情報を選択し、該情報の情報識別番号および、鍵生成用情報を取り出す（SD 1）。次いで、乱数発生部 24 で乱数 R を生成した後（SD 2）、情報センタ装置 1 に接続して（SD 3）、前記情報に対応する情報識別番号、乱数 R、端末識別番号蓄積部 22 より取り出した端末識別番号および、鍵生成用情報と共に情報センタ装置 1 に送信する（SD 4）。

【0034】情報センタ装置 1 では、鍵生成部 14 で前記受信した情報識別番号、端末識別番号、及び鍵生成用情報のうち前記情報を暗号化した時と同じパラメータを利用して秘密関数により計算した復号鍵 K s を生成する（SD 5）。この後、暗号化部 15 で、秘密鍵群蓄積部 13 より取り出した該端末識別番号 I D i に対応する端末秘密鍵 K i により、前記復号鍵 K s と乱数 R の結合ビット列 K s || R を暗号化し（SD 6）、端末装置 2 に送信する（SD 7）。

【0035】端末装置 2 では、前記情報センタ装置 1 からの受信情報を復号部 27 で秘密鍵蓄積部 26 より取り出した端末の秘密鍵 K i で復号して（SD 8）、乱数 R と復号鍵 K s を取り出し、該乱数 R と送信前に端末装置 2 で生成した乱数を比較する（SD 9）。この比較の結果、乱数が一致しない場合には、情報の復号を禁止する（SD 10）。また、一致した場合には、復号部 27 で該復号鍵 K s により情報蓄積部 23 内の該暗号化デジタル情報を復号した後（SD 11）、前記乱数及び復号鍵を消去する（SD 12）。

【0036】なお、以上の第 1 及び第 2 の実施例はいずれも、I S D N などの公衆通信回線を利用する場合の例で示したが、専用線などコネクションレスの回線にも適用できる。その場合は、図 2、図 4、図 6、図 8 のそれぞれで「情報センタ装置と回線接続」の動作は不要である。

【0037】また、以上の実施例は、端末装置 2 が情報センタ装置 1 にデジタル情報を指定して情報の送信を依頼する例で示したが、情報センタ装置 1 で選択したデジタル情報を端末装置 2 で受信するシステムにも適用可能である。

【0038】さらに、本発明は、コンピュータソフトウェアのみならず、全てに暗号化デジタル情報の通信利用による配送の際に適用できることはいうまでもない。

【0039】

10 【発明の効果】以上説明したように本発明の請求項 1 記載のデジタル情報保護システムによれば、暗号化されたデジタル情報本体を通信回線利用により配送した後、情報を利用する際に、1 回のみ利用可能な復号鍵を通信回線により配送すると共に、端末装置において乱数を生成して情報センタ装置に送信して、情報センタ装置では復号鍵と乱数を暗号化して端末装置に返送しているので、端末装置と情報センタ装置間の送受信情報を盗聴して同一のトランザクションを生成する疑似センタにより同一デジタル情報の課金なしの不正利用を防止することができる。さらに、個人のプライバシーを侵害することもない。

20 【0040】また、請求項 2 記載のデジタル情報保護方法によれば、暗号化されたデジタル情報本体を通信回線利用により配送した後、情報を利用する際に、1 回のみ利用可能な復号鍵を通信回線により配送すると共に、端末装置において乱数を生成して情報センタ装置に送信して、情報センタ装置では復号鍵と乱数を暗号化して端末装置に返送しているので、端末装置と情報センタ装置間の送受信情報を盗聴して同一のトランザクションを生成する疑似センタにより同一デジタル情報の課金なしの不正利用を防止できると共に、個人のプライバシーを侵害することもない。

30 【0041】さらに、請求項 3 によれば、上記の効果に加えて、情報識別番号だけでなく端末識別番号、作成年月日等のパラメータを組み合わせて暗号鍵を生成しているため、各同一のデジタル情報に対して常に異なる復号鍵を生成することができるので、安全性の高い鍵配送システムが可能となる大きな利点がある。また、情報センタ装置に複数の端末装置に対して各デジタル情報ごとの暗号鍵を蓄積しておく必要がないため、安全性と情報センタ装置の資源の有効利用を図ることができる。

【図面の簡単な説明】

【図 1】本発明の第 1 の実施例のデジタル情報保護システムを示す構成図

【図 2】本発明の第 1 の実施例におけるデジタル情報の受信・蓄積動作手順を示すフローチャート

【図 3】第 1 の実施例における端末装置の情報蓄積部内の情報内容を示す図

50 【図 4】第 1 の実施例におけるデジタル情報を利用する際の動作手順を示すフローチャート

【図5】第1の実施例における情報センタ装置の秘密鍵群蓄積部の情報内容を示す図

【図6】本発明の第2の実施例におけるデジタル情報の受信・蓄積動作手順を示すフローチャート

【図7】第2の実施例における端末装置の情報蓄積部内の情報内容を示す図

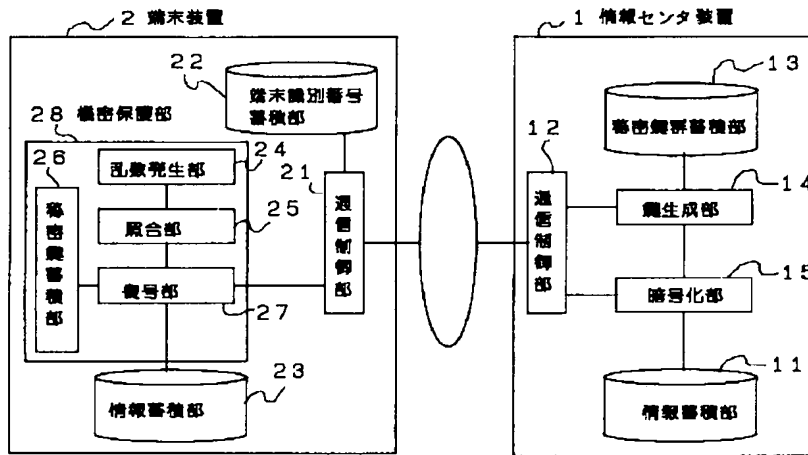
【図8】第2の実施例におけるデジタル情報を利用する際の動作手順を示すフローチャート

*

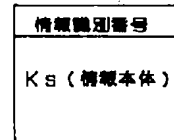
* 【符号の説明】

1…情報センタ装置、2…端末装置、11…情報蓄積部、12…通信制御部、13…秘密鍵群蓄積部、14…鍵生成部、15…暗号化部、21…通信制御部、22…端末識別番号蓄積部、23…情報蓄積部、24…乱数発生部、25…照合部、26…秘密鍵蓄積部、27…復号部、28…機密保護部。

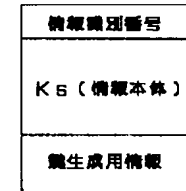
【図1】



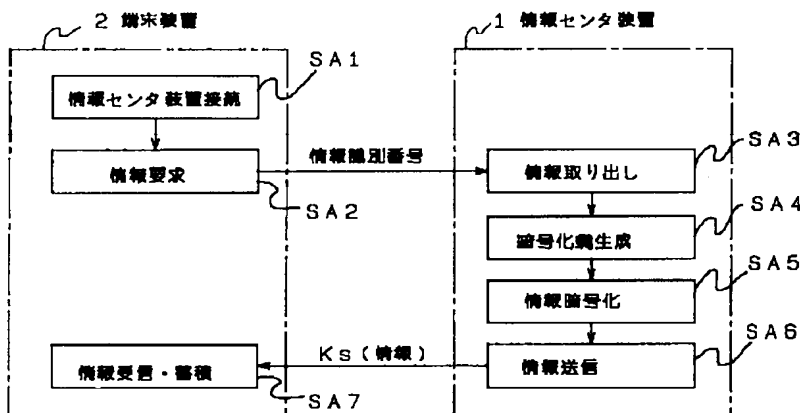
【図3】



【図7】



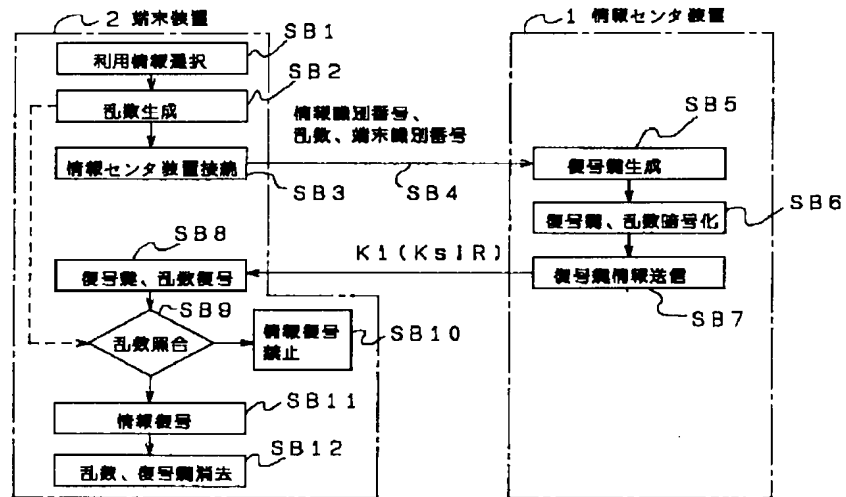
【図2】



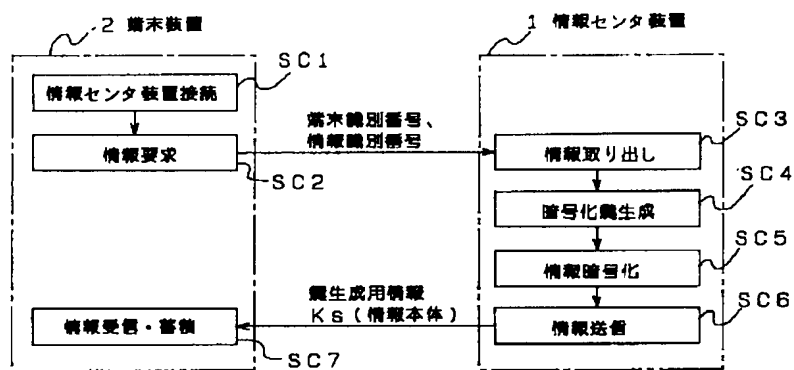
【図5】

端末識別番号	端末秘密鍵
ID1	K1
ID2	K2
ID3	K3
:	:

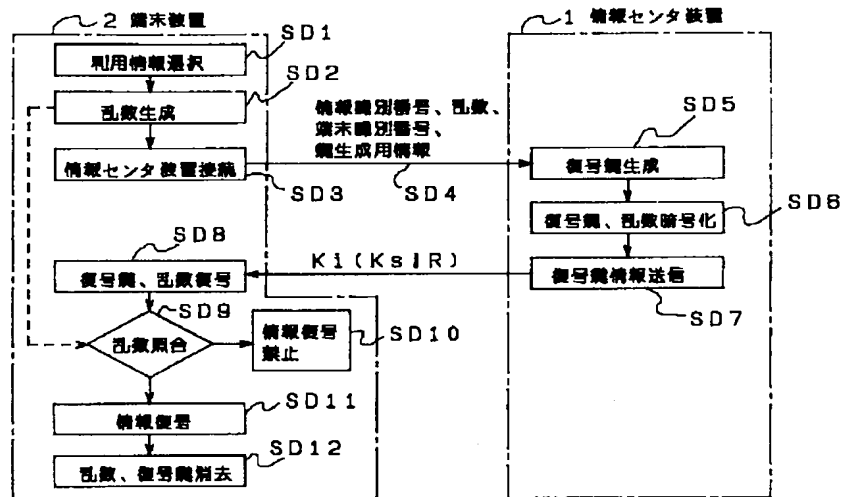
【図4】



【図6】



【図 8】



フロントページの続き

(72)発明者 神田 雅透
東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内
(72)発明者 松田 伸広
神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内

(72)発明者 関谷 邦彦
神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内
(72)発明者 矢幡 明樹
東京都日野市旭が丘3丁目1番地の1 株
式会社東芝日野工場内